3

訂正有り

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-187888

⑤Int. Cl.³	識別記号	庁内整理番号	⑬公開　平成2年(1990)7月24日
G 06 K 17/00	S	6711-5B	
G 09 C 1/00		7368-5B	

審査請求　未請求　請求項の数 4　(全16頁)

⑭発明の名称　認証方式

⑳特　願　平1-8010
㉒出　願　平1(1989)1月17日

㉑発明者　飯島　康雄　神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉔代理人　弁理士　鈴江　武彦　外3名

明　細　書

1．発明の名称

認証方式

2．特許請求の範囲

（1）第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、

第2の電子装置から第1の電子装置に対し第1のデータおよび、その第1のデータを暗号化するためのキーデータを指定する指定データを送信する手段と、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づき1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化する手段と、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する手段と

を具備したことを特徴とする認証方式。

（2）第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、

第2の電子装置から第1の電子装置に対し第1のデータおよび、その第1のデータを暗号化するためのキーデータおよび暗号化アルゴリズムを指定する指定データを送信する手段と、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化する手段と、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する手段と

を具備したことを特徴とする認証方式。

（3）第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり、

第２の電子装置から第１の電子装置に対し第１のデータおよび、その部度内容の異なる第２のデータを送信する手段と、

第１の電子装置において、前記第１のデータおよび第２のデータを受信すると、その受信した第２のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第１のデータを暗号化する手段と、

第１の電子装置において、前記第１のデータを全て受信した後に、その暗号化データのうち一部のデータを第２の電子装置に送信する手段と

を具備したことを特徴とする認証方式。

（４）第１の電子装置は、少なくとも１つのメモリ部と、このメモリ部に受信した第１のデータを記憶する手段を更に具備したことを特徴とする請求項１ないし３記載の認証方式。

３．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、たとえばＩＣカード内のメモリ部に対しデータを書込む際、その書込みデータの正当性を確認する認証方式に関する。

（従来の技術）

近年、新たな携帯可能なデータ記憶媒体として、消去可能な不揮発性メモリおよび、これらを制御するＣＰＵなどの制御素子を有するＩＣチップを内蔵した、いわゆるＩＣカードが注目されている。

従来、このようなＩＣカードを利用したＩＣカードシステム（たとえばショッピングシステムやクレジットシステムなど）においては、ＩＣカード（実際はＩＣカード内のメモリ部）へのデータ書込み処理、特に取引データを書込む際、センタ（ホストコンピュータ）に送られる取引データの正当性がセンタ側で確認できなかった。

このため、端末装置からデータを書込む命令をＩＣカードが受信すると、ＩＣカード内でキーデータおよび暗号化アルゴリズムを使用して書込みデータを暗号化し、その暗号化データのうち一部のデータを端末装置に送り、これを受信した端末装置では、その暗号化データおよび書込みデータをそれぞれセンタに送り、センタで、これらの各データにより書込みデータの正当性を確認する認証方式が考えられている。

（発明が解決しようとする課題）

しかし、このような認証方式では、ＩＣカードが多目的利用されるにつれ、複数のアプリケーションで使用されることになった場合、正当性を確認するための各アプリケーションが保管している確認用のキーデータを異ならせる方が、各アプリケーション間のセキュリティを確保するためには有効である。

そこで、本発明は、たとえば複数のアプリケーションでＩＣカードが使用されることになっても、各アプリケーションで使用する正当性確認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる認証方式を提供することを目的とする。

また、上記した認証方式では、書込みデータ、キーデータおよび暗号化アルゴリズムが同一であれば、ＩＣカードから出力される暗号化データも同一となってしまい、本来の取引データの正当性確認が困難となるという問題があった。

そこで、本発明は、同一の書込みデータ、キーデータおよび暗号化アルゴリズムであっても、書込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる認証方式を提供することを目的とする。

［発明の構成］

（課題を解決するための手段）

本発明の認証方式は、第１の電子装置と、この第１の電子装置との間で通信可能な第２の電子装置とからなり、第２の電子装置から第１の電子装置に対し第１のデータおよび、その第１のデータを暗号化するためのキーデータを指定する指定データを送信する手段と、第１の電子装置において、前記第１のデータおよび指定データを受信すると、あらかじめ用意された少なくとも１つのキーデータの中から前記受信した指定データに基づ

き１つのキーデータを選択し、この選択したキーデータを使用して前記受信した第１のデータを暗号化する手段と、第１の電子装置において、前記第１のデータを全て受信した後に、その暗号化データのうち一部のデータを第２の電子装置に送信する手段とを具備している。

また、本発明の認証方式は、第１の電子装置と、この第１の電子装置との間で通信可能な第２の電子装置とからなり、第２の電子装置から第１の電子装置に対し第１のデータおよび、その第１のデータを暗号化するためのキーデータおよび暗号化アルゴリズムを指定する指定データを送信する手段と、第１の電子装置において、前記第１のデータおよび指定データを受信すると、あらかじめ用意された少なくとも１つのキーデータおよび少なくとも１つの暗号化アルゴリズムの中から前記受信した指定データに基づき１つのキーデータおよび１つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第１のデータを暗号化する手段と、第１の電子装置において、前記第１のデータを全て受信した後に、その暗号化データのうち一部のデータを第２の電子装置に送信する手段とを具備している。

さらに、本発明の認証方式は、第１の電子装置と、この第１の電子装置との間で通信可能な第２の電子装置とからなり、第２の電子装置から第１の電子装置に対し第１のデータおよび、その都度内容の異なる第２のデータを送信する手段と、第１の電子装置において、前記第１のデータおよび第２のデータを受信すると、その受信した第２のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第１のデータを暗号化する手段と、第１の電子装置において、前記第１のデータを全て受信した後に、その暗号化データのうち一部のデータを第２の電子装置に送信する手段とを具備している。

（作用）

本発明は、ＩＣカード（第１の電子装置）の内部に保有している複数のキーデータのうち１つのキーデータを端末装置（第２の電子装置）から指定し、この指定したキーデータを用いて書込みデータを暗号化することにより、たとえば複数のアプリケーションでＩＣカードが使用されることになっても、各アプリケーションで使用する正当性確認用のキーデータを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

また、本発明は、ＩＣカード（第１の電子装置）の内部に保有している複数のキーデータおよび複数の暗号化アルゴリズムのうち１つのキーデータおよび１つの暗号化アルゴリズムを端末装置（第２の電子装置）から指定し、この指定したキーデータおよび暗号化アルゴリズムを用いて書込みデータを暗号化することにより、たとえば複数のアプリケーションでＩＣカードが使用されることになっても、各アプリケーションで使用する正当性確認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

さらに、本発明は、端末装置（第２の電子装置）からＩＣカード（第１の電子装置）に送信された、その都度内容の異なるデータをパラメータとして書込みデータを暗号化することにより、同一の書込みデータ、キーデータおよび暗号化アルゴリズムであっても、書込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる。

（実施例）

以下、本発明の一実施例について図面を参照して説明する。

第８図は、本発明に係るＩＣカード（第１の電子装置）と、その上位装置である端末装置（第２の電子装置）と、その上位装置であるセンタ（ホストコンピュータ）とのシステム構成図である。

ＩＣカード（第１の電子装置）１０は、各種データを記憶するためのメモリ部１１、乱数データを発生する乱数発生部１２、データの暗号化を行なう暗号化部１３、後述する端末装置２０と通信するためのコンタクト部１４、およびこれらを制

御するＣＰＵなどの制御素子１５などから構成されていて、これらのうちメモリ部１１、乱数発生部１２、暗号化部１３および制御素子１５は、たとえば１つのＩＣチップ（あるいは複数のＩＣチップ）で構成されてＩＣカード本体内に埋設されている。

メモリ部１１は、たとえばＥＥＰＲＯＭなどの不揮発性メモリによって構成されており、第２図に示すように、エリア定義テーブル（領域）１６とデータファイル（領域）１７とに大きく分割されている。そして、データファイル１７内は、図示するように複数のエリア１８，…に分割定義されるもので、これら各エリア１８…はエリア定義テーブル１６内のエリア定義情報１９によってそれぞれ定義される。

ここに、エリア定義情報１９は、たとえばエリアを指定する識別情報としてのエリア番号（ＡＩＤ）、エリアが割当てられているメモリ上の先頭アドレス情報、エリアの容量を規定するサイズ情報および属性情報を対応付けたデータ列である。なお、属性情報は、たとえば１バイトで構成されていて、そのＭＳＢが「０」であれば暗号化データ書込みエリアであり、「１」であれば入力データ書込みエリアであることを示している。

端末装置（第２の電子装置）２０は、ＩＣカード１０を取扱う機能を有し、各種データを記憶するメモリ部２１、乱数データを発生する乱数発生部２２、データの暗号化を行なう暗号化部２３、データの入力などを行なうキーボード部２４、データを表示する表示部２５、ＩＣカード１０と通信するためのコンタクト部２６、センタ（ホストコンピュータ）３０と通信回線３１を介してオンラインで通信する通信制御部２７、およびこれらを制御するＣＰＵなどの制御部２８から構成されている。

次に、このような構成において、本発明に係る認証方式を第１図を用いて詳細に説明する。なお、端末装置２０のメモリ部２１には、図示するようなキーデータリストおよびキーデータ番号（ＫＩＤ）リストが格納されているものとする。

キーデータリストはキーデータ番号とキーデータとを対応付けたリストであり、ＫＩＤリストはキーデータを指定するキーデータ番号のみがリスト化されたものである。一方、ＩＣカード１０は、独自にキーデータリストを有しており、これはカード発行時などで内部のメモリ部１１に登録（記憶）される。

さて、まずステップ１～ステップ８によって、ＩＣカード１０と端末装置２０との間で行なわれる相互認証のプロセスを説明する。まず、ステップ１において、端末装置２０は、乱数発生部２２によって乱数データＲ１を生成し、認証準備コマンドＥＸＣＨによって、これをＩＣカード１０に送信する。このとき、端末装置２０がＩＣカード１０を認証するために使用するキーデータのキーデータ番号（ＫＩＤ－Ｍ）、および端末装置２０がサポートしている暗号化アルゴリズム（ＡＬＧ）の指定データをも合わせて送信する。

次に、ステップ２において、ＩＣカード１０は、認証準備コマンドＥＸＣＨを受信すると、乱数発生部１２によって乱数データＲ２を生成し、それを認証準備コマンドＥＸＣＨに対するレスポンスｅｘｃｈとして端末装置２０に送信する。このとき、ＩＣカード１０は、端末装置２０を認証するために使用するキーデータのキーデータ番号（ＫＩＤ－Ｎ）を自身のもつキーリストより見付けだし、かつ指定された暗号化アルゴリズム（ＡＬＧ）を自身がサポートしているかを判断し、これをａｌｇとして乱数データＲ２と合わせて端末装置２０に送信する。

もしこのとき、端末装置２０から指定されたキーデータ番号（ＫＩＤ－Ｍ）がキーリストに存在しなかったり、あるいはＩＣカード１０が端末装置２０を認証するために使用するキーデータ番号（ＫＩＤ－Ｎ）がキーリストに存在しなかったり、あるいは指定された暗号化アルゴリズムをサポートしていなかった場合には、その旨を端末装置２０に通知する。

次に、ステップ３において、端末装置２０は、ＩＣカード１０から指定された暗号化キーデータ

のキーデータ番号（ＫＩＤ－Ｎ）を自己が所有するキーリストから捜し出し、対応するキーデータ（ＮＮＮＮＮ）を取出す。そして、暗号化部２３によって、暗号化アルゴリズムＡＬＧ（＝ａｌｇ）を使用してキーデータ（ＮＮＮＮＮ）によりＩＣカード１０からの乱数データＲ２を暗号化し、その結果、すなわち暗号化データＣ２を認証コマンドＡＵＴＨによってＩＣカード１０に送信する。なお、図中、Ｅは暗号化を実現する機能ボックスを示す。

次に、ステップ４において、ＩＣカード１０が認証コマンドＡＵＴＨを受信すると、ＩＣカード１０は、先に送信した暗号化キーデータのキーデータ番号（ＫＩＤ－Ｎ）を自己が所有するキーリストより捜し出し、対応するキーデータ（ＮＮＮＮＮ）を取出す。そして、暗号化部１３によって、認証準備コマンドＥＸＣＨで指定された暗号化アルゴリズム（ＡＬＧ）を使用してキーデータ（ＮＮＮＮＮ）により乱数データＲ２を暗号化し、暗号化データＣ２Ｘを得る。

次に、ステップ５において、ＩＣカード１０は、先に受信した認証コマンドＡＵＴＨ中の暗号化データＣ２とステップ４で生成した暗号化データＣ２Ｘとを比較し、その比較結果Ｙ／Ｎを得る。

次に、ステップ６において、ＩＣカード１０は、認証準備コマンドＥＸＣＨで端末装置２０から指定された暗号化キーデータのキーデータ番号（ＫＩＤ－Ｍ）に対応するキーデータ（ＭＭＭＭＭ）を取出す。次に、暗号化部１３によって、暗号化アルゴリズム（ＡＬＧ）を使用してキーデータ（ＭＭＭＭＭ）により乱数データＲ１を暗号化し、暗号化データＣ１を得る。そして、この暗号化データＣ１とステップ５による比較結果Ｙ／Ｎを、認証コマンドＡＵＴＨに対するレスポンスａｕｔｈとして端末装置２０に送信する。

次に、ステップ７において、端末装置２０がレスポンスａｕｔｈを受信すると、端末装置２０は、先に送信した暗号化キーデータのキーデータ番号（ＫＩＤ－Ｍ）に対応するキーデータ（ＭＭＭＭＭ）を取出す。そして、暗号化部２３によって、暗号化アルゴリズム（ＡＬＧ）を使用してキーデータ（ＭＭＭＭＭ）により端末装置２０からの乱数データＲ１を暗号化し、暗号化データＣ１Ｘを得る。

次に、ステップ８において、端末装置２０は、レスポンスａｕｔｈによって受信した暗号化データＣ１とステップ７で生成した暗号化データＣ１Ｘとを比較し、この比較結果とレスポンスａｕｔｈにより受信したステップ５によるＩＣカード１０での比較結果とにより、以降のシステム処理の決定を行なう。

次に、ステップ９～ステップ２３によって、端末装置２０からＩＣカード１０に対しデータを書込むとともに、書込み処理の正当性を確認するプロセスを説明する。まず、ステップ９において、端末装置２０は、書込みコマンドＷＲＩＴＥによりデータを書込む要求をＩＣカード１０に送信する。このとき、端末装置２０は、ＩＣカード１０内のメモリ部１１に対する書込み対象エリアのエリア番号（ＡＩＤ－Ａ）、書込みデータのバイト数（Ｌ－１）、および書込みデータ（Ｍ１）のうちＩＣカード１０が入力データとして受信し得るバイト数に分割した最初の分割データ（Ｍ１－１）をＩＣカード１０に送信する。

次に、ステップ１０において、ＩＣカード１０は、書込みコマンドＷＲＩＴＥによって受信したエリア番号（ＡＩＤ－Ａ）が付されたエリアを第２図のエリア定義テーブル１６から見付ける。もし見付からなければ、エリア番号未定義を意味するステータスを書込みコマンドＷＲＩＴＥに対するレスポンスｗｒｉｔｅによって端末装置２０に送信する。もし見付かれば、先に認証準備コマンドＥＸＣＨ、または後述する暗号化準備コマンドＳＲＮＤが正常終了されているかをチェックする。

このチェックの結果、もし正常終了されていなければ、実行条件不備ステータスをレスポンスｗｒｉｔｅによって端末装置２０に送信する。上記チェックの結果、正常終了されていれば、ＩＣカード１０は、先の認証準備コマンド

ＥＸＣＨによって通知された乱数データＲ１とＩＣカード１０の内部で所有するカード固有値とにより初期データＲ１′を生成する。

次に、ステップ１１において、ＩＣカード１０は、先に認証準備コマンドＥＸＣＨで指定された暗号化アルゴリズム（ＡＬＧ）を使用して、初期データＲ１′および先に認証準備コマンドＥＸＣＨによって通知されたキーデータ番号（ＫＩＤ－Ｍ）に対応するキーデータ（ＭＭＭＭＭ）により書込みデータ（Ｍ１－１）を暗号化し、暗号化データ（Ｃ１－１）を得る。次に、アクセス対象となっているエリア番号（ＡＩＤ－Ａ）のエリアの属性情報を参照することにより、メモリ部１１への書込みデータを入力データ（Ｍ１－１）にするか暗号化データ（Ｃ１－１）にするかを決定し、書込み処理を行なう。そして、端末装置２０に対し次の書込みデータを要求するためのレスポンス`ｎｂ´を送信する。

次に、レスポンス`ｎｂ´を受信すると、端末装置２０は、ステップ１２において、次の書込みデータ（Ｍ１－２）をＩＣカード１０に送信する。次に、ステップ１３において、次の書込みデータ（Ｍ１－２）を受信すると、ＩＣカード１０は、再び暗号化アルゴリズム（ＡＬＧ）を使用して、先に生成した暗号化データ（Ｃ１－１）の最終の８バイトデータおよびキーデータ番号（ＫＩＤ－Ｍ）に対応するキーデータ（ＭＭＭＭＭ）により書込みデータ（Ｍ１－２）を暗号化し、暗号化データ（Ｃ１－２）を得る。次に、ステップ１１と同様に、メモリ部１１への書込みデータを入力データ（Ｍ１－２）にするか暗号化データ（Ｃ１－２）にするかを決定し、選択的にエリアへの書込み処理を行なう。そして、端末装置２０に対し次の書込みデータを要求するためのレスポンス`ｎｂ´を送信する。

以下、ステップ１２，１３と同様の処理動作を繰返し行なう。

さて、ステップ１４において、端末装置２０が分割データの最終データ（Ｍ１－ｎ）をＩＣカード１０に送信すると、ステップ１５において、ＩＣカード１０は同様の書込み処理を行なう。そして、最終的に生成された暗号化データ（Ｃ１－ｎ）のうち最終８バイトを確認情報（ＡＣ１）とし、書込みコマンドＷＲＩＴＥに対するレスポンスｗｒｉｔｅによって端末装置２０に送信する。

すなわち、上記処理においては、あらかじめ相互認証手順で端末装置２０がＩＣカード１０を認証するために、ＩＣカード１０に対して指定したキーデータ（ＭＭＭＭＭ）、暗号化アルゴリズム（ＡＬＧ）および乱数データ（Ｒ１）を使用して、書込みデータＭ１に対する確認情報（ＡＣ１）が得られている。

次に、上記とは異なるキーデータ、暗号化アルゴリズムおよび乱数データにより確認情報を得るプロセスをステップ１６～ステップ２０によって説明する。まず、ステップ１６において、端末装置２０は、乱数発生部２２によって新規の乱数データＲ３を生成し、暗号化準備コマンドＳＲＮＤによって、これをＩＣカード１０に送信する。このとき、ＩＣカード１０が確認情報を生成するのに使用するキーデータのキーデータ番号（ＫＩＤ－Ａ）、および暗号化アルゴリズム（ＡＬＧ´）を合わせて送信する。

次に、ステップ１７において、ＩＣカード１０は、暗号化準備コマンドＳＲＮＤを受信すると、キーデータ番号（ＫＩＤ－Ａ）を自身が所有するキーリストから見付けだし、対応するキーデータ（ＡＡＡＡＡ）を得て、レスポンスｓｒｎｄを端末装置２０に送信する。

次に、ステップ１８において、端末装置２０は、書込みコマンドＷＲＩＴＥによりデータを書込む要求をＩＣカード１０に送信する。このとき、端末装置２０は、ＩＣカード１０内のメモリ部１１に対する書込み対象エリアのエリア番号（ＡＩＤ－Ｂ）、書込みデータのバイト数（Ｌ－２）、および書込みデータ（Ｍ２）を送信する。なお、本ステップ１８では、書込みデータ（Ｍ２）のバイト数は、ＩＣカード１０が入力データとして受信し得るバイト数である。

次に、ステップ１９において、ＩＣカード１０

は、ステップ１０と同様にしてエリア番号（ＡＩＤ－Ｂ）が付されたエリアを第２図におけるエリア定義テーブル１６から見付ける。そして、次にＩＣカード１０として、先に暗号化準備コマンドＳＲＮＤ（または認証準備コマンドＥＸＣＨ）が正常終了されているか否かをチェックする。もし、正常終了されているとすると、ＩＣカード１０は、暗号化準備コマンドＳＲＮＤによって通知された乱数データＲ３とＩＣカード１０の内部で所有するカード固有値とにより初期データＲ３′を生成する。

次に、ステップ２０において、ＩＣカード１０は、先に暗号化準備コマンドＳＲＮＤで指定された暗号化アルゴリズム（ＡＬＧ′）を使用して、初期データＲ３′および先に暗号化準備コマンドＳＲＮＤにより通知されたキーデータ番号（ＫＩＤ－Ａ）に対応するキーデータ（ＡＡＡＡＡ）により書込みデータ（Ｍ２）を暗号化し、暗号化データＣ２を得る。次に、アクセス対象となっているエリア番号（ＡＩＤ－Ｂ）のエリアの属性情報を参照することにより、メモリ部１１への書込みデータを入力データ（Ｍ２）にするか暗号化データ（Ｃ２）にするかを決定し、書込み処理を行なう。そして、端末装置２０に対し、暗号化データ（Ｃ２）のうち最終８バイトのデータを確認情報（ＡＣ２）として、書込みコマンドＷＲＩＴＥに対するレスポンスｗｒｉｔｅによって送信する。

なお、ＩＣカード１０は、第２図のエリア定義テーブル１６内の先頭アドレス情報およびサイズ情報によりメモリ部１１内の物理的位置を確認する。先頭アドレス情報は対応するエリアの先頭アドレス値であり、サイズ情報は先頭アドレス値からのエリアの容量を規定している。また、属性情報は１バイトで構成され、そのＭＳＢが「０」であれば暗号化データ書込みエリアであり、「１」であれば入力データ書込みエリアであることを示す。

次に、ステップ２１において、端末装置２０は、ＩＣカード１０へのデータ書込みを終了すると、書込みデータ（Ｍ１，Ｍ２）に対応する乱数データ（Ｒ１，Ｒ３）、キーデータ番号（ＫＩＤ－Ｍ，ＫＩＤ－Ａ）、確認情報（ＡＣ１，ＡＣ２）、および使用アルゴリズム指定値（ＡＬＧ，ＡＬＧ′）により、データ書込み処理リストを作成する。なお、このときカード固有値もリストに対応付けておく。そして、この作成したリストをセンタ３０へ送信する。

次に、ステップ２２において、センタ３０は、端末装置２０からのリストを受信すると、そのリストから書込みデータ（Ｍ１）を取出し、対応するキーデータ番号（ＫＩＤ－Ｍ）により、キーデータ（ＭＭＭＭＭ）を自身が所有するキーリストから見付けだし、かつ自身が所有する取引きリストで対応付けられている乱数データ（Ｒ１）および暗号化アルゴリズム（ＡＬＧ）により確認情報（ＡＣＩＸ）を生成する。

そして、ステップ２３において、リストで対応付けられた確認情報（ＡＣ１）とステップ２２で生成した確認情報（ＡＣ１Ｘ）とを比較し、両者が一致していればセンタ３０は書込みデータ（Ｍ１）に対する書込み処理の正当性を確認する。

書込みデータ（Ｍ２）以降についても、ステップ２２，２３と同様な処理により正当性を確認する。

次に、ＩＣカード１０としての動作を第７図を用いて説明する。まず、制御端子１５は、端末装置２０からの制御信号によって電気的活性化を経た後、アンサー・ツー・リセットと称する初期応答データを端末装置２０へ出力する（Ｓ１）。そして、制御端子１５は、認証準備コマンド完了フラグおよび暗号化準備コマンド完了フラグをオフし（Ｓ２）、命令データ待ち状態に移る。

この状態で、命令データを受信すると（Ｓ３）、制御端子１５は、まず、この命令データが第３図に示す認証準備コマンドＥＸＣＨであるか否かを判断し（Ｓ４）、もしそうでないと判断すると次のフローに移る。

ステップＳ４において、認証準備コマンドＥＸＣＨであると判断すると、制御端子１５は、

認証準備コマンド中のキーデータ番号（ＫＩＤ）フィールドの内容をピックアップし、メモリ部１１内に登録されているキーリストから同一のキーデータ番号を見付ける（Ｓ５）。

そして、もしキーデータ番号が見付からなければ（Ｓ６）、制御素子１５は、キーデータ指定エラーステータスを出力し（Ｓ７）、命令データ待ち状態に戻る。もし、キーデータ番号が見付かれば（Ｓ６）、制御素子１５は、対応するキーデータを内部ＲＡＭ上の第１キーバッファにセーブする（Ｓ８）。

次に、制御素子１５は、認証準備コマンド中の暗号化アルゴリズム指定データ（ＡＬＧ）フィールドを参照することにより、メモリ上に登録されている暗号化アルゴリズムであるか否かをチェックする（Ｓ９）。このチェックの結果、指定された暗号化アルゴリズムが存在しない場合（Ｓ１０）、制御素子１５は、指定アルゴリズムエラーステータスを出力し（Ｓ１１）、命令データ待ち状態に戻る。上記チェックの結果、指定された暗号化アルゴリズムが存在する場合（Ｓ１０）、制御素子１５は、その暗号化アルゴリズムの番号をセーブしておく（Ｓ１２）。

次に、制御素子１５は、認証準備コマンド中の乱数データ（Ｒ１）を内部ＲＡＭ上の第１乱数バッファにセーブし（Ｓ１３）、その後、先のキーリストからＩＣカード認証用キーデータのキーデータ番号（ＫＩＤ′）を見付ける（Ｓ１４）。

そして、もしキーデータ番号が見付からなければ（Ｓ１５）、制御素子１５は、キーデータ未登録エラーステータスを出力し（Ｓ１６）、命令データ待ち状態に戻る。もし、キーデータ番号が見付かれば（Ｓ１５）、制御素子１５は、対応するキーデータを内部ＲＡＭ上の第２キーバッファにセーブする（Ｓ１７）。

次に、制御素子１５は、乱数発生部１２によって乱数データＲ２を生成し、内部ＲＡＭ上の第２乱数バッファにセーブする（Ｓ１８）。そして、制御素子１５は、認証準備コマンド完了フラグをオンし（Ｓ１９）、かつ、生成した乱数データＲ２を先のキーデータ番号（ＫＩＤ′）および認証準備コマンド中の暗号化アルゴリズム指定データ（ＡＬＧ）フィールドの内容とともに、認証準備コマンドＥＸＣＨに対するレスポンスｅｘｃｈとして端末装置２０に出力し（Ｓ２０）、命令データ待ち状態に戻る。

ステップＳ４において、認証準備コマンドＥＸＣＨでないと判断すると、制御素子１５は、第４図に示す認証コマンドＡＵＴＨであるか否かを判断し（Ｓ２１）、もしそうでないと判断すると次のフローへ移る。

ステップ２１において、認証コマンドＡＵＴＨであると判断すると、制御素子１５は、認証準備コマンド完了フラグがオンされているか否かを判断し（Ｓ２２）、もしオフであれば実行条件不備エラーステータスを出力し（Ｓ２３）、命令データ待ち状態に戻る。

ステップ２２において、認証準備コマンド完了フラグがオンであれば、制御素子１５は、暗号化部１３により、第２キーバッファの内容を暗号化のキーデータとして第２乱数バッファの内容を暗号化する（Ｓ２４）。このときの暗号化アルゴリズムは、セーブされた暗号化アルゴリズム番号に対応する暗号化アルゴリズムを使用する。

そして、制御素子１５は、上記暗号化の結果と認証コマンドＡＵＴＨで送られた入力データとを比較し（Ｓ２５）、その比較結果に応じて一致フラグをオンまたはオフする（Ｓ２６～Ｓ２８）。

次に、制御素子１５は、暗号化部１３により、第１キーバッファの内容を暗号化のキーデータとして第１乱数バッファの内容を暗号化する（Ｓ２９）。このときの暗号化アルゴリズムも上記同様のものを使用する。そして、制御素子１５は、この暗号化の結果を先の一致フラグの内容とともに、認証コマンドＡＵＴＨに対するレスポンスａｕｔｈとして端末装置２０に出力し（Ｓ３０）、命令データ待ち状態に戻る。

ステップＳ２１において、認証コマンドＡＵＴＨでないと判断すると、制御素子１５は、第５図に示す暗号化準備コマンドＳＲＮＤである

か否かを判断し（Ｓ３１）、もしそうでないと判断すると次のフローへ移る。

ステップ３１において、暗号化準備コマンドＳＲＮＤであると判断すると、制御素子１５は、暗号化準備コマンド中のキーデータ番号（ＫＩＤ）フィールドの内容をピックアップし、メモリ部１１内に登録されているキーリストから同一のキーデータ番号を見付ける（Ｓ３２）。

そして、もしキーデータ番号が見付からなければ（Ｓ３３）、制御素子１５は、キーデータ指定エラーステータスを出力し（Ｓ３４）、命令データ待ち状態に戻る。もし、キーデータ番号が見付かれば（Ｓ３３）、制御素子１５は、対応するキーデータを内部ＲＡＭ上の第１キーバッファにセーブする（Ｓ３５）。

次に、制御素子１５は、暗号化準備コマンド中の暗号化アルゴリズム指定データ（ＡＬＧ）フィールドを参照することにより、メモリ上に登録されている暗号化アルゴリズムであるか否かをチェックする（Ｓ３６）。このチェックの結果、指定された暗号化アルゴリズムが存在しない場合（Ｓ３７）、制御素子１５は、指定アルゴリズムエラーステータスを出力し（Ｓ３８）、命令データ待ち状態に戻る。上記チェックの結果、指定された暗号化アルゴリズムが存在する場合（Ｓ３７）、制御素子１５は、その暗号化アルゴリズムの番号をセーブしておく（Ｓ３９）。

次に、制御素子１５は、暗号化準備コマンド中の乱数データ（Ｒ３）を内部ＲＡＭ上の第１乱数バッファにセーブし（Ｓ４０）、その後、暗号化準備コマンド完了フラグをオンし（Ｓ４１）、かつ暗号化準備コマンド完了ステータスを端末装置２０に出力し（Ｓ４２）、命令データ待ち状態に戻る。

ステップＳ３１において、暗号化準備コマンドＳＲＮＤでないと判断すると、制御素子１５は、第６図（ａ）または（ｂ）に示す書込みコマンドＷＲＩＴＥであるか否かを判断し（Ｓ５１）、もしそうでないと判断すると、他のコマンド（たとえばデータの読出しコマンド）であるか否かの判断を行ない、対応する処理へ移行する。

ステップＳ５１において、書込みコマンドＷＲＩＴＥであると判断すると、制御素子１５は、その書込みコマンドが第６図（ａ）の形式か（ｂ）の形式かを判断し（Ｓ５２）、第６図（ａ）の書込みコマンドであれば、認証準備コマンド完了フラグおよび暗号化準備コマンド完了フラグを参照し（Ｓ５３）、どちらかでもオフとなっていれば（Ｓ５４）、条件不備ステータスを出力し（Ｓ５５）、命令データ待ち状態に戻る。もしどちらかのフラグがオンとなっていれば（Ｓ５４）、制御素子１５は、書込みコマンド中のデータ部の内容を内部ＲＡＭ上の第２ライトバッファにセーブする（Ｓ５６）。

ステップＳ５２において、第６図（ｂ）の書込みコマンドであれば、制御素子１５は、内部で保持している書込みコマンド継続フラグがオンか否かを判断する（Ｓ５７）。もしオフとなっていれば、制御素子１５は、要求エラーステータスを出力し（Ｓ５８）、命令データ待ち状態に戻る。もしオンとなっていれば、制御素子１５は、内部ＲＡＭ上のデータセーブバッファの内容に書込みコマンド中のデータ部の内容（入力データ）を付加し、内部ＲＡＭ上の第２ライトバッファにセーブする（Ｓ５９）。

そして、制御素子１５は、書込みコマンド中のデータ部の内容（入力データ）のみを内部ＲＡＭ上の第１ライトバッファにセーブする（Ｓ６０）。

次に、制御素子１５は、第６図（ａ）または（ｂ）の書込みコマンドによって送られた入力データに書込み後続データが存在するか否かをチェックし（Ｓ６１）、書込み後続データが存在すれば後続フラグをオンし（Ｓ６２）、書込み後続データが存在しなければ後続フラグをオフする（Ｓ６３）。

次に、制御素子１５は、内部ＲＡＭ上の第２ライトバッファ内のデータのバイト数が例えば「８」の倍数であるか否かをチェックし（Ｓ６４）、もしそうであればステップＳ７０に移行する。もしそうでなければ、制御素子１５は、後続フラグを

参照してオフとなっていれば（Ｓ６５）、内部ＲＡＭ上の第２ライトバッファ内のデータにパディング処理（たとえば"２０"Ｈｅｘデータを後ろに付加）し（Ｓ６６）、「８」の倍数分のデータを生成してステップＳ７０に移行する。

ステップＳ６５において、後続フラグがオンとなっていれば、制御素子１５は、「８」の倍数分のデータを残し、残りのデータを内部ＲＡＭ上のデータセーブバッファに移動する（Ｓ６７）。すなわち、たとえば第２ライトバッファに１８バイトのデータが存在すれば、１６バイトのデータのみを残して残りの２バイトはデータセーブバッファに移動する。このとき、内部ＲＡＭ上の第２ライトバッファ内が空となっていなければ（Ｓ６８）、ステップＳ７０に移行する。

ステップＳ６８において、内部ＲＡＭ上の第２ライトバッファ内が空となっていれば（たとえば第２ライトバッファ内に７バイトのデータがあれば、先の処理で第２ライトバッファ内のデータ全てがデータセーブバッファに移動されるため、結果として第２ライトバッファは空となる）、制御素子１５は、今回アクセスしているエリアが書込み時に暗号化するエリアか否かを判断する（Ｓ６９）。そして、もしそうでなければステップＳ７１に移行し、もしそうであればステップＳ７９に移行する。

さて、ステップＳ７０において、制御素子１５は、暗号化部１３により、内部ＲＡＭ上の第２ライトバッファ内のデータを例えばＣＢＣモードで暗号化する。このとき、継続フラグがオフとなっていれば、内部ＲＡＭ上の第１乱数バッファの内容にカード固有値を排他的論理和したものを、また継続フラグがオンとなっていれば、前回の書込みで暗号化したデータの最終８バイトをそれぞれ初期値として、今回のＣＢＣモード暗号化に使用する。また、このときのキーデータは第１キーバッファの内容を使用し、暗号化アルゴリズムは保持されている暗号化アルゴリズム番号により選択的に使用する。そして、この処理が終了するとステップＳ７１に移行する。

ステップＳ７１において、制御素子１５は、継続フラグがオンされているか否かを判断し、オンされていればアクセス対象エリアが暗号化を要するエリアか否かを判断する（Ｓ７２）。もし暗号化を要するエリアでなければ、制御素子１５は、内部ＲＡＭ上の第１ライトバッファの内容に書込みコマンド中の書込みデータのバイト数ＬＸを付加して、メモリ部１１のアクセス対象エリア内にデータを書込む（Ｓ７３）。また、もし暗号化を要するエリアであれば、制御素子１５は、書込みデータのバイト数ＬＸよりも大なる「８」の倍数で、最少の値をＬＸ'とし、これを第２ライトバッファ内のデータを付加して書込む（Ｓ７４）。

ステップＳ７１において、継続フラグがオンされていれば、制御素子１５は、アクセス対象エリアが暗号化を要するエリアか否かを判断する（Ｓ７５）。もし暗号化を要するエリアでなければ、制御素子１５は、内部ＲＡＭ上の第１ライトバッファの内容を先に書込んだデータに追加して書込む（Ｓ７６）。また、もし暗号化を要するエリアであれば、制御素子１５は、内部ＲＡＭ上の第２ライトバッファの内容を同様に書込む（Ｓ７７）。

さて、データを書込んだ後は、制御素子１５は、後続フラグがオンされているか否かを判断し（Ｓ７８）、オンされていれば継続フラグをオンしてレスポンス"ｎｂ"を出力し（Ｓ７９）、命令データ待ち状態に戻る。もし、後続フラグがオフとなっていれば、制御素子１５は、内部ＲＡＭ上の第２ライトバッファの内容の最終８バイトを出力して継続フラグをオフし（Ｓ８０）、命令データ待ち状態に戻る。

このように、ＩＣカードの内部に保有している複数のキーデータおよび複数の暗号化アルゴリズムのうち１つのキーデータおよび１つの暗号化アルゴリズムを端末装置から指定し、この指定したキーデータおよび暗号化アルゴリズムを用いて書込みデータを暗号化することにより、複数のアプリケーションでＩＣカードが使用されることになっても、各アプリケーションで使用する正当性確

認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

なお、端末装置２０からＩＣカード１０に送信される乱数データＲ１，Ｒ３は、その都度内容が同一のデータであってもよいが、その都度内容の異なるデータとすることにより、同一の書込みデータ、キーデータおよび暗号化アルゴリズムであっても、書込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる。

この場合、端末装置２０内において、たとえば時計回路を設け、この時計回路から発生する時間情報を用いて乱数データＲ１，Ｒ３を生成することにより、容易にその都度内容の異なるデータを得ることができる。

［発明の効果］

以上詳述したように本発明の認証方式によれば、たとえば複数のアプリケーションでＩＣカードが使用されることになっても、各アプリケーションで使用する正当性確認用のキーデータおよび暗号化アルゴリズムを選択的に運用でき、アプリケーション間のセキュリティを確保することが可能となる。

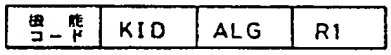
また、本発明の認証方式によれば、同一の書込みデータ、キーデータおよび暗号化アルゴリズムであっても、書込み時間が異なれば出力される暗号化データも異なるものになり、正当性の確認が容易となる。

４．図面の簡単な説明

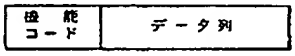
図は本発明の一実施例を説明するためのもので、第１図はＩＣカードと端末装置との間の相互認証手順および端末装置からＩＣカードへのデータ書込み手順を示す図、第２図はメモリ部の構成を示す図、第３図は認証準備コマンドのフォーマット例を示す図、第４図は認証コマンドのフォーマット例を示す図、第５図は暗号化準備コマンドのフォーマット例を示す図、第６図は書込みコマンドのフォーマット例を示す図、第７図はＩＣカードの動作を説明するフローチャート、第８図はＩＣカードと端末装置とセンタとのシステム構成図である。

１０…ＩＣカード（第１の電子装置）、１１…メモリ部、１２…乱数発生部、１３…暗号化部、１４…コンタクト部、１５…制御端子、２０…端末装置（第２の電子装置）、２１…メモリ部、２２…乱数発生部、２３…暗号化部、２６…コンタクト部、２７…通信制御部、２８…制御部、３０…センタ（ホストコンピュータ）。

出願人代理人　弁理士　鈴　江　武　彦

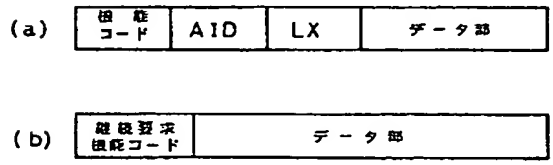


第３図

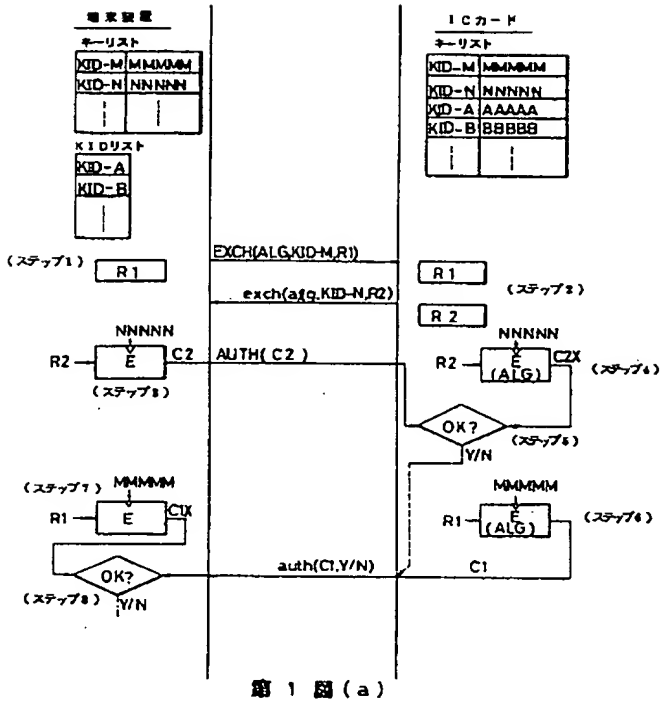


第４図

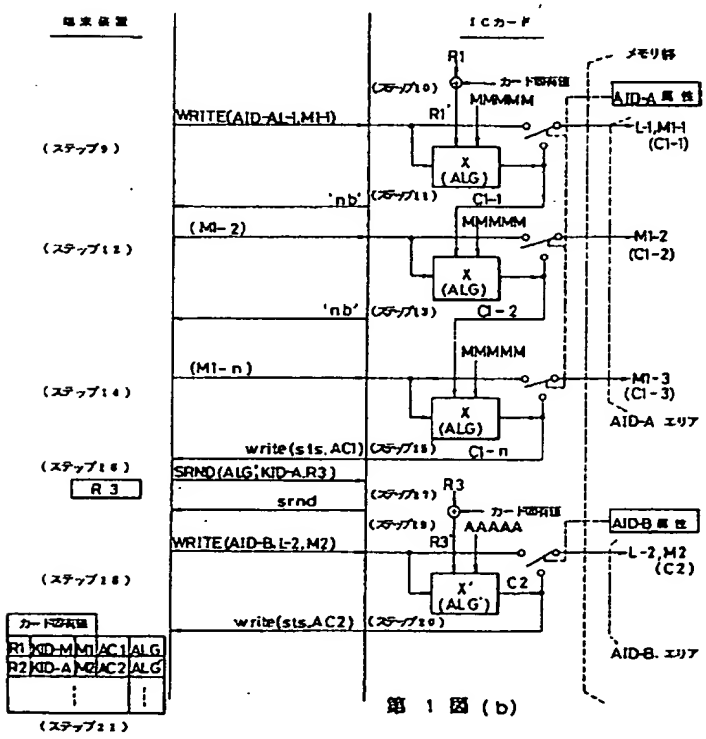
第５図



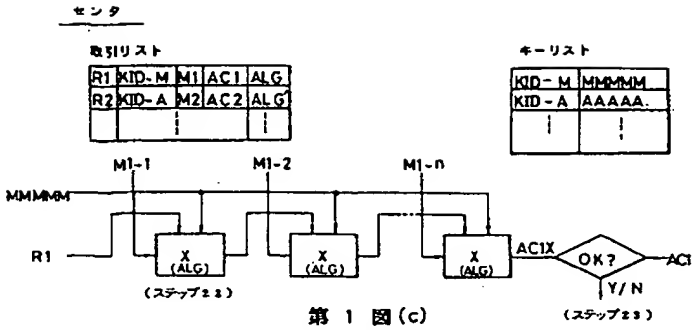
第６図


端末装置
キーリスト
KID-M MMMMM
KID-N NNNNN
KIDリスト
KID-A
KID-B
ICカード
キーリスト
KID-M MMMMM
KID-N NNNNN
KID-A AAAAA
KID-B BBBBB
(ステップ1)
R1
EXCH(ALG,KID-M,R1)
R1
(ステップ2)
exch(alg,KID-N,R2)
R2
NNNNN
E
C2
AUTH(C2)
R2
NNNNN
E
(ALG)
C2X
(ステップ4)
(ステップ3)
OK?
(ステップ5)
Y/N
(ステップ7)
MMMMM
R1
E
C1X
MMMMM
R1
E
(ALG)
(ステップ6)
OK?
(ステップ8)
Y/N
auth(C1,Y/N)
C1

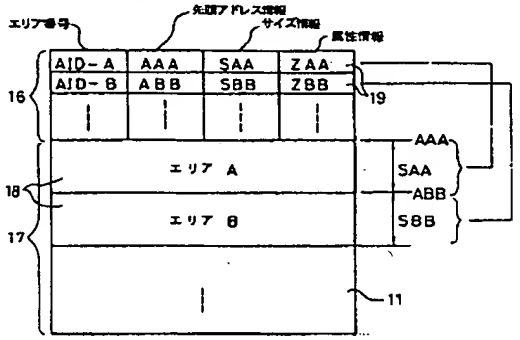
第 1 図 (a)


端末装置
ICカード
メモリ特
R1
(ステップ10)
カード固有値
MMMMM
AID-A 属性
WRITE(AID-A,L-1,M1-1)
R1'
L-1,M1-1
(C1-1)
(ステップ9)
X
(ALG)
'nb'
(ステップ11)
C1-1
(M1-2)
MMMMM
(ステップ12)
M1-2
(C1-2)
X
(ALG)
'nb'
(ステップ13)
C1-2
MMMMM
(M1-n)
M1-3
(C1-3)
(ステップ14)
X
(ALG)
AID-A エリア
write(sts,AC1)
(ステップ15)
C1-n
(ステップ16)
SRND(ALG,KID-A,R3)
R3
srnd
(ステップ17)
R3
(ステップ19)
カード固有値
AAAAA
AID-B 属性
WRITE(AID-B,L-2,M2)
R3
L-2,M2
(C2)
(ステップ18)
X'
(ALG')
C2
write(sts,AC2)
(ステップ20)
AID-B エリア
カード内容
R1 KID-M M1 AC1 ALG
R2 KID-A M2 AC2 ALG
(ステップ21)

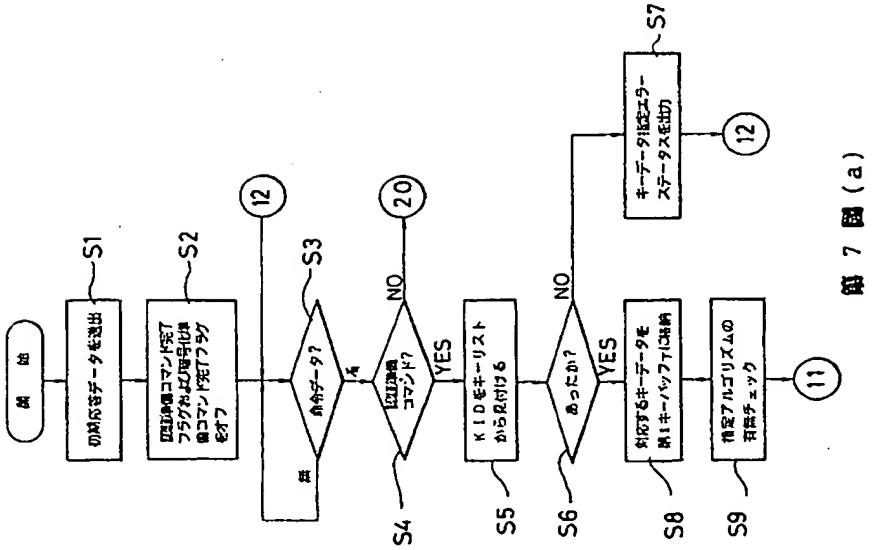
第 1 図 (b)



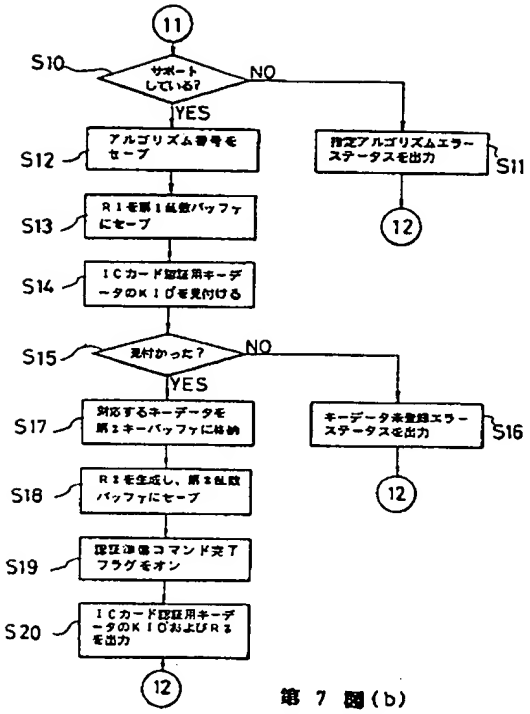
第 1 図(c)



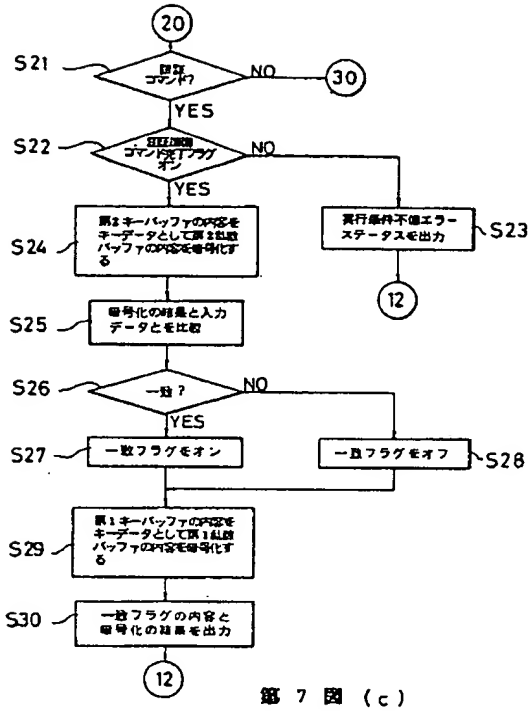
第 2 図



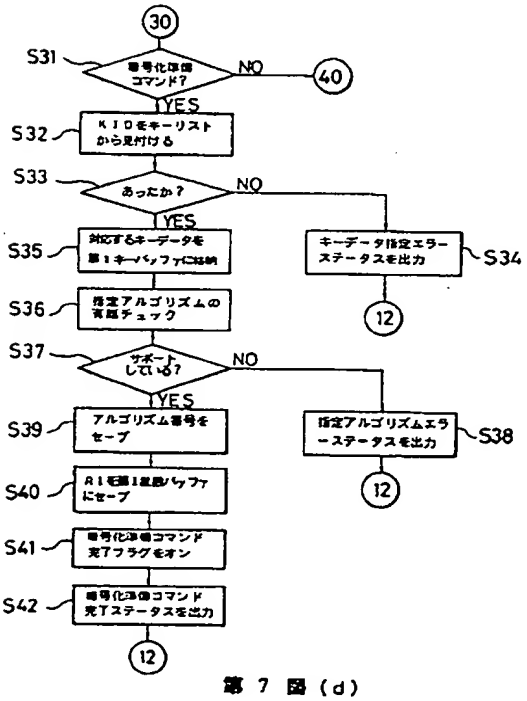
第 7 図 (a)



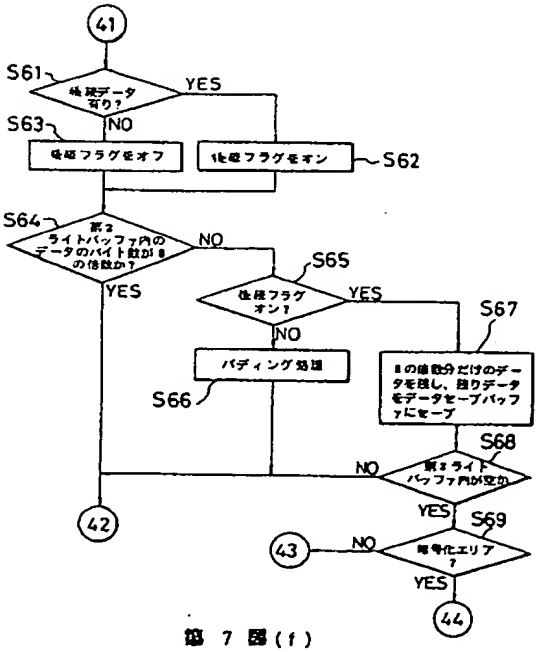
第 7 図 (b)



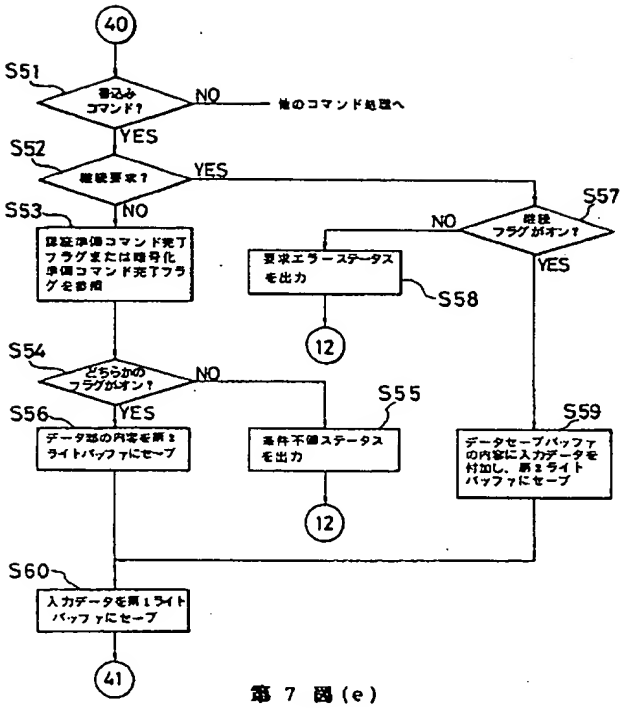
第 7 図 (c)



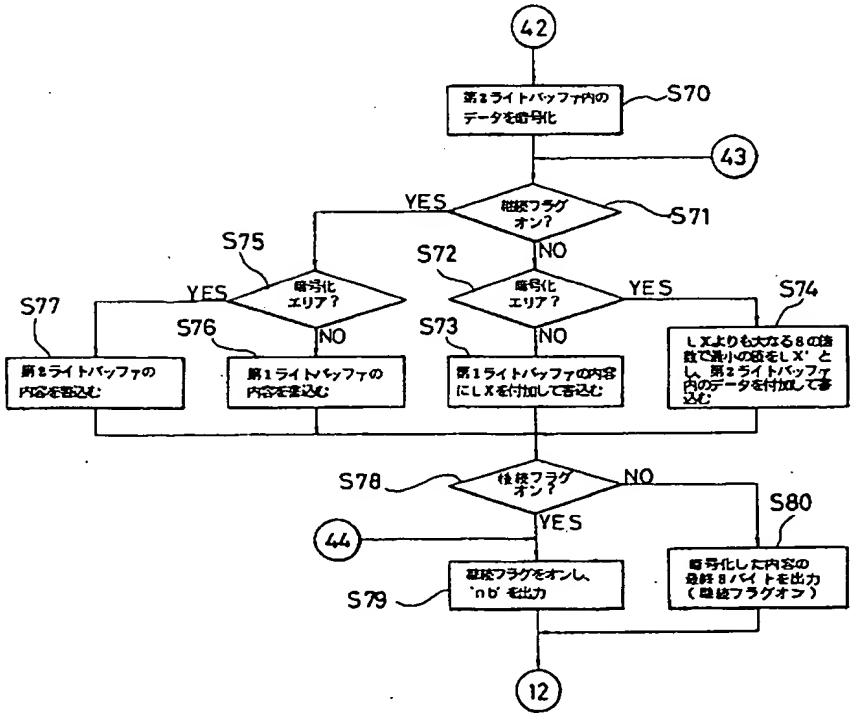
第 7 図 (d)



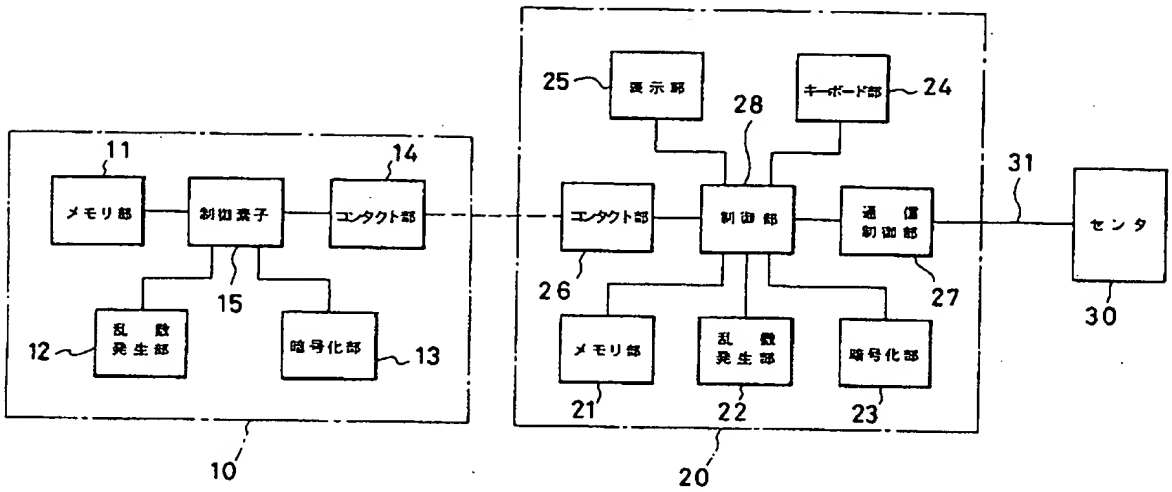
第 7 図 (f)


40
S51
書込みコマンド?
NO
他のコマンド処理へ
YES
S52
継続要求?
YES
NO
S53
障害準備コマンド完了フラグまたは暗号化準備コマンド完了フラグを参照
S57
継続フラグがオン?
NO
YES
要求エラーステータスを出力
S58
12
S54
どちらかのフラグがオン?
NO
YES
S55
S56
データ部の内容を第2ライトバッファにセーブ
条件不備ステータスを出力
12
S59
データセーブバッファの内容に入力データを付加し、第2ライトバッファにセーブ
S60
入力データを第1ライトバッファにセーブ
41

第 7 図 (e)


42
第2ライトバッファ内のデータを暗号化
S70
43
YES
継続フラグオン?
S71
NO
S75
暗号化エリア?
YES
NO
S72
暗号化エリア?
YES
NO
S74
S77
S76
S73
第2ライトバッファの内容を書込む
第1ライトバッファの内容を書込む
第1ライトバッファの内容にLXを付加して書込む
LXよりも大なる8の倍数で最小の数をLX'とし、第2ライトバッファ内のデータを付加して書込む
S78
継続フラグオン?
NO
YES
S80
44
継続フラグをオンし、'nb'を出力
S79
暗号化した内容の最終8バイトを出力(継続フラグオフ)
12

第 7 図 (g)


11
メモリ部
制御素子
14
コンタクト部
15
12
乱数発生部
暗号化部
13
10
25
表示部
28
キーボード部
24
コンタクト部
制御部
通信制御部
31
センタ
26
27
30
メモリ部
乱数発生部
暗号化部
21
22
23
20

第 8 図

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成８年（１９９６）１２月２４日

【公開番号】特開平２－１８７８８８
【公開日】平成２年（１９９０）７月２４日
【年通号数】公開特許公報２－１８７９
【出願番号】特願平１－８０１０
【国際特許分類第６版】
G06K 17/00
G09C 1/00
【ＦＩ】
G06K 17/00 S 7623-5B
G09C 1/00 7259-5J

手 続 補 正 書

平成 年 月 日

特許庁長官 深 川 佑 二 殿

1. 事件の表示
特 願 平 1 － 8 0 1 0 号

2. 発明の名称
認 証 方 式

3. 補正をする者
事件との関係 特許出願人
(307) 株 式 会 社 東 芝

4. 代 理 人
東 京 都 千 代 田 区 霞 が 関 3 丁 目 7 番 2 号
鈴 榮 内 外 国 特 許 事 務 所 内
〒100 電話03（3502）3181（大代表）
(5847) 弁理士 鈴 江 武 彦

5. 自発補正

6. 補正の対象
明 細 書

7. 補正により増加する請求項の数 1

8. 補正の内容
（1）特許請求の範囲を別紙の通り訂正する。
（2）明細書の第6頁第12行目ないし第8頁第17行目にわたって「本発明の認証方式は、……具備している。」とあるを下記の通り訂正する。

記

本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータを指定する指定データを送信し、第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づき1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化し、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信することを特徴としている。

また、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータ、および、暗号化アルゴリズムを指定する指定データを送信し、第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信することを特徴としている。

また、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、第2の電子装置から第1の電子装置に対し第1のデータ、および、その処理内容の異なる第

2のデータを送信し、第1の電子装置において、前記第1のデータおよび第2のデータを受信すると、その受信した第2のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信することを特徴としている。

さらに、本発明の認証方式は、第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子との間で行なわれる認証方式において、第1の電子装置および第2に電子装置のそれぞれにおいて複数のキーデータを記憶しておき、第1の電子装置から第2の電子装置に対してキーデータを指定する第1のキー指定データおよび第1のデータを送信し、第2の電子装置から第1の電子装置に対してキーデータを指定する第2のキー指定データおよび第2のデータを送信し、第2の電子装置では、この第1のキー指定データにより指定されたキーデータを読出して、このキーデータを用いて第1のデータを暗号化して第1の認証データを作成し、第2の電子装置から第1の電子装置に対して第1の認証データを送信し、第1の電子装置において送信した第1のキー指定データに対応するキーデータを読出して、このキーデータを用いて第1のデータを暗号化して第2の認証データを作成し、第1の電子装置において第2の認証データと第2の電子装置から送信されてきた第1の認証データとを比較して第2の電子装置の正当性を確認し、第1の電子装置において受信した第2のキー指定データにより指定されたキーデータを読出して、このキーデータを用いて第2のデータを暗号化して第3の認証データを作成し、第2の電子装置の正当性が確認された場合は、第2の認証データと第1の認証データとの比較結果および第1の電子装置において作成した第3の認証データを第2の電子装置へ送信し、第2の電子装置の正当性が確認されなかった場合は、第2の認証データと第1の認証データとの比較結果を第1の電子装置から第2の電子装置に対して送信することを特徴としている。

2. 特許請求の範囲

(1) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、

第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータを指定する指定データを送信し、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータの中から前記受信した指定データに基づき1つのキーデータを選択し、この選択したキーデータを使用して前記受信した第1のデータを暗号化し、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する

ことを特徴とする認証方式。

(2) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、

第2の電子装置から第1の電子装置に対し第1のデータ、および、その第1のデータを暗号化するためのキーデータ、および、暗号化アルゴリズムを指定する指定データを送信し、

第1の電子装置において、前記第1のデータおよび指定データを受信すると、あらかじめ用意された少なくとも1つのキーデータおよび少なくとも1つの暗号化アルゴリズムの中から前記受信した指定データに基づき1つのキーデータおよび1つの暗号化アルゴリズムを選択し、この選択したキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する

ことを特徴とする認証方式。

(3) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子装置との間で行なわれる認証方式において、

第2の電子装置から第1の電子装置に対し第1のデータ、および、その都度内容の異なる第2のデータを送信し、

第1の電子装置において、前記第1のデータおよび第2のデータを受信すると、その受信した第2のデータ、あらかじめ用意されたキーデータおよび暗号化アルゴリズムを使用して前記受信した第1のデータを暗号化し、

第1の電子装置において、前記第1のデータを全て受信した後に、その暗号化データのうち一部のデータを第2の電子装置に送信する

ことを特徴とする認証方式。

(4) 第1の電子装置は、少なくとも1つのメモリ部と、このメモリ部に受信した第1のデータを記憶する手段を更に具備したことを特徴とする前項1ないし3記載の認証方式。

(5) 第1の電子装置と、この第1の電子装置との間で通信を行なう第2の電子との間で行なわれる認証方式において、

第1の電子装置および第2に電子装置のそれぞれにおいて複数のキーデータを記憶しておき、

第1の電子装置から第2の電子装置に対してキーデータを指定する第1のキー指定データおよび第1のデータを送信し、

第2の電子装置から第1の電子装置に対してキーデータを指定する第2のキー指定データおよび第2のデータを送信し、

第2の電子装置では、この第1のキー指定データにより指定されたキーデータを読出して、このキーデータを用いて第1のデータを暗号化して第1の認証データを作成し、

第2の電子装置から第1の電子装置に対して第1の認証データを送信し、

第1の電子装置において送信した第1のキー指定データに対応するキーデータを読出して、このキーデータを用いて第1のデータを暗号化して第2の認証データを作成し、

第1の電子装置において第2の認証データと第2の電子装置から送信されてきた第1の認証データとを比較して第2の電子装置の正当性を確認し、

第1の電子装置において受信した第2のキー指定データにより指定されたキーデータを読出して、このキーデータを用いて第2のデータを暗号化して第3の認証データを作成し、

第2の電子装置の正当性が確認された場合は、第2の認証データと第1の認証データとの比較結果および第1の電子装置において作成した第3の認証データを第2の電子装置へ送信し、

第2の電子装置の正当性が確認されなかった場合は、第2の認証データと第1の認証データとの比較結果を第1の電子装置から第2の電子装置に対して送信する

ことを特徴とする認証方式。

出願人代理人　弁理士　鈴　江　武　彦